

National Cyber Alert System

Cyber Security Bulletin SB10-018

[Archive](#)

Vulnerability Summary for the Week of January 11, 2010

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat adobe -- acrobat_reader	The U3D implementation in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors, related to an "array boundary issue," a different vulnerability than CVE-2009-2994.	2010-01-13	10.0	CVE-2009-3953 CONFIRM
adobe -- acrobat adobe -- acrobat_reader	The 3D implementation in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors, related to a "DLL-loading vulnerability."	2010-01-13	10.0	CVE-2009-3954 CONFIRM
adobe -- acrobat adobe -- acrobat_reader	Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors, related to a "memory corruption vulnerability."	2010-01-13	10.0	CVE-2009-3955 CONFIRM
adobe -- acrobat adobe -- acrobat_reader	The default configuration of Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, does not properly support the Enhanced Security feature, which has unspecified impact and attack vectors, related to a "script injection vulnerability."	2010-01-13	10.0	CVE-2009-3956 CONFIRM
adobe -- acrobat adobe -- acrobat_reader	Buffer overflow in the Download Manager in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors.	2010-01-13	10.0	CVE-2009-3958 CONFIRM

adobe -- acrobat adobe -- acrobat_reader	Integer overflow in the U3D implementation in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to execute arbitrary code via unspecified vectors.	2010-01-13	10.0	CVE-2009-3959 CONFIRM
corephp -- com_jphoto	SQL injection vulnerability in the JPhoto (com_jphoto) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a category action to index.php.	2010-01-12	7.5	CVE-2009-4598 XF BID MISC SECUNIA MISC OSVDB
fernando_soares -- com_mamboleto	PHP remote file inclusion vulnerability in mamboleto.php in the Fernando Soares Mamboleto (com_mamboleto) component 2.0 RC3 for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2010-01-12	7.5	CVE-2009-4604 XF BID MISC MISC
gnu -- glibc	nis/nss_nis/nis-pwd.c in the GNU C Library (aka glibc or libc6) 2.7 and Embedded GLIBC (EGLIBC) 2.10.2 adds information from the passwd.adjunct.byname map to entries in the passwd map, which allows remote attackers to obtain the encrypted passwords of NIS accounts by calling the getpwnam function.	2010-01-14	7.5	CVE-2010-0015 MLIST MLIST MLIST MLIST CONFIRM MISC MLIST MLIST CONFIRM
ibm -- domino_web_access ibm -- lotus_domino ibm -- lotus_inotes	Unspecified vulnerability in IBM Lotus iNotes (aka Domino Web Access or DWA) before 229.131 for Domino 8.0.x has unknown impact and attack vectors, aka SPR SDOY7RHBNH.	2010-01-09	10.0	CVE-2009-4594 CONFIRM CONFIRM CONFIRM
ibm -- tivoli_access_manager_for_e- business sun -- java_system_access_manager sun -- java_system_identity_server sun -- opensso_enterprise	Unspecified vulnerability in Sun Java System Identity Manager (aka IdM) 8.1.0.5 and 8.1.0.6, when Sun Java System Access Manager, OpenSSO Enterprise 8.0, or IBM Tivoli Access Manager is used, allows remote attackers to obtain administrative access via unknown vectors.	2010-01-14	9.3	CVE-2010-0311 CONFIRM
ibm -- tivoli_directory_server	The do_extendedOp function in ibmslapd in IBM Tivoli Directory Server (TDS) 6.2 on Linux allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted SecureWay 3.2 Event Registration Request (aka a 1.3.18.0.2.12.1 request).	2010-01-14	7.8	CVE-2010-0312 SECTRACK MISC
icculus -- alien_arena	Stack-based buffer overflow in the M_AddToServerList function in client/menu.c in Red Planet Arena Alien Arena 7.30 allows remote attackers to execute arbitrary code via a packet with a crafted server description to UDP port 27901 followed by a packet with a long print command.	2010-01-13	10.0	CVE-2009-3637 FEDORA FEDORA VUPEN BID BUGTRAQ MISC SECUNIA SECUNIA

				SECUNIA CONFIRM
intel -- e1000 linux -- kernel linux -- kernel	drivers/net/e1000/e1000_main.c in the e1000 driver in the Linux kernel 2.6.32.3 and earlier handles Ethernet frames that exceed the MTU by processing certain trailing payload data as if it were a complete frame, which allows remote attackers to bypass packet filters via a large packet with a crafted payload. NOTE: this vulnerability exists because of an incorrect fix for CVE-2009-1385.	2010-01-12	7.8	CVE-2009-4536 CONFIRM BID REDHAT REDHAT MLIST MLIST MLIST SECTRACK SECUNIA SECUNIA CONFIRM MISC MISC
intel -- e1000 linux -- kernel linux -- kernel	drivers/net/r8169.c in the r8169 driver in the Linux kernel 2.6.32.3 and earlier does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to (1) cause a denial of service (temporary network outage) via a packet with a crafted size, in conjunction with certain packets containing A characters and certain packets containing E characters; or (2) cause a denial of service (system crash) via a packet with a crafted size, in conjunction with certain packets containing '\0' characters, related to the value of the status register and erroneous behavior associated with the RxMaxSize register. NOTE: this vulnerability exists because of an incorrect fix for CVE-2009-1389.	2010-01-12	7.8	CVE-2009-4537 CONFIRM BID REDHAT REDHAT MLIST MLIST MLIST MISC SECTRACK SECUNIA CONFIRM MLIST MISC MISC
intel -- e1000 linux -- kernel linux -- kernel	drivers/net/e1000e/netdev.c in the e1000e driver in the Linux kernel 2.6.32.3 and earlier does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to have an unspecified impact via crafted packets, a related issue to CVE-2009-4537.	2010-01-12	10.0	CVE-2009-4538 CONFIRM BID REDHAT REDHAT MLIST MLIST MLIST SECTRACK SECUNIA
joomshark -- com_jsjobs	Multiple SQL injection vulnerabilities in the JS Jobs (com_jsjobs) component 1.0.5.6 for Joomla! allow remote attackers to execute arbitrary SQL commands via (1) the md parameter in an employer view_company action to index.php or (2) the oi parameter in an employer view_job action to index.php.	2010-01-12	7.5	CVE-2009-4599 XF BID MISC MISC
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_7 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows 2000 SP4; Windows XP SP2 and SP3; Windows Server 2003 SP2; Windows Vista Gold, SP1, and SP2; Windows Server 2008 Gold, SP2, and R2; and Windows 7 allows remote attackers to execute arbitrary code via compressed data that represents a crafted EOT font, aka "Microtype Express Compressed Fonts Integer Flaw in the LZCOMP Decompressor Vulnerability."	2010-01-13	9.3	CVE-2010-0018 MS

mit -- kerberos	Multiple integer underflows in the (1) AES and (2) RC4 decryption functionality in the crypto library in MIT Kerberos 5 (aka krb5) 1.3 through 1.6.3, and 1.7 before 1.7.1, allow remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code by providing ciphertext with a length that is too short to be valid.	2010-01-13	10.0	CVE-2009-4212 CONFIRM CONFIRM
netartmedia -- media_real_estate_portal	SQL injection vulnerability in realestate20/loginaction.php in NetArt Media Real Estate Portal 2.0 allows remote attackers to execute arbitrary SQL commands via the Email parameter (aka the username field). NOTE: some of these details are obtained from third party information.	2010-01-12	7.5	CVE-2009-4600 XF BID MISC SECUNIA OSVDB
netartmedia -- media_real_estate_portal	SQL injection vulnerability in realestate20/loginaction.php in NetArt Media Real Estate Portal 2.0 allows remote attackers to execute arbitrary SQL commands via the Password parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2010-01-14	7.5	CVE-2009-4613 SECUNIA OSVDB
oracle -- database_server	Unspecified vulnerability in the Oracle OLAP component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	2010-01-12	9.0	CVE-2009-3415 CERT
oracle -- database_server	Unspecified vulnerability in the Listener component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2010-01-12	10.0	CVE-2010-0071 CERT
oracle -- secure_backup	Unspecified vulnerability in the Oracle Secure Backup component in Oracle Secure Backup 10.2.0.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	2010-01-12	10.0	CVE-2010-0072 CERT
oracle -- bea_product_suite	Multiple vulnerabilities in the JRockit component in BEA Product Suite R27.6.5 using JRE/JDK 1.4.2, 5, and 6 allow remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: this CVE identifier overlaps CVE-2009-3867, CVE-2009-3868, CVE-2009-3869, CVE-2009-3871, CVE-2009-3872, CVE-2009-3873, CVE-2009-3874, CVE-2009-3875, CVE-2009-3876, and CVE-2009-3877.	2010-01-12	10.0	CVE-2010-0079 CERT
overlandstorage -- snap_server_410 overlandstorage -- guardianos	The command line interface in Overland Storage Snap Server 410 with GuardianOS 5.1.041 runs the "less" utility with a higher-privileged uid than the CLI user and without sufficient restriction on shell escapes, which allows local users to gain privileges using the "!" character within less to access a privileged shell.	2010-01-13	7.2	CVE-2009-4607 XF BID BUGTRAQ MISC
phpwares -- php_inventory	Multiple SQL injection vulnerabilities in index.php in PHP Inventory 1.2 allow (1) remote authenticated users to execute arbitrary SQL commands via the user_id parameter in a users details action, and allow remote attackers to execute arbitrary SQL commands via the (2) user (username) and (3) pass (password) parameters. NOTE: some of these details are obtained from third party information.	2010-01-12	7.5	CVE-2009-4597 XF MISC SECUNIA MISC

south_river_technologies -- webdrive	South River Technologies WebDrive 9.02 build 2232 installs the WebDrive Service without a security descriptor, which allows local users to (1) stop the service via the stop command, (2) execute arbitrary commands as SYSTEM by using the config command to modify the binPath variable, or (3) restart the service via the start command.	2010-01-13	7.2	CVE-2009-4606 XF VUPEN BUGTRAQ SECUNIA MISC OSVDB
sun -- java_system_directory_server	The core_get_proxyauth_dn function in ns-slapd in Sun Java System Directory Server Enterprise Edition 7.0 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted LDAP Search Request message.	2010-01-14	7.8	CVE-2010-0313 XF VUPEN BID SECTRACK SECUNIA MISC
tibco -- runtime_agent	The (1) domainutility and (2) domainutilitycmd components in TIBCO Domain Utility in TIBCO Runtime Agent (TRA) before 5.6.2, as used in TIBCO ActiveMatrix BusinessWorks and other products, set weak permissions on domain properties files, which allows local users to obtain domain administrator credentials, and gain privileges on all domain systems, via unspecified vectors.	2010-01-14	7.2	CVE-2010-0184 VUPEN CONFIRM CONFIRM BID SECUNIA

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acme -- mini_httpd	mini_httpd 1.19 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4490 MISC BUGTRAQ
acme -- thttpd	thttpd 2.25b0 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4491 MISC BUGTRAQ
adobe -- acrobat adobe -- acrobat_reader	Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, might allow attackers to cause a denial of service (NULL pointer dereference) via unspecified vectors.	2010-01-13	5.0	CVE-2009-3957 CONFIRM
aol -- aolserver	AOLserver 4.5.1 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4494 MISC BID BUGTRAQ
apple -- safari	Apple Safari allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then reading the document.styleSheets[o].href property value.	2010-01-14	5.0	CVE-2010-0314 MISC

boa -- boa	Boa 0.94.14rc21 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4496 MISC BUGTRAQ
bts-gi.net -- read_excel	Unrestricted file upload vulnerability in upload.php in BTS-GI Read excel 1.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in an unspecified directory. NOTE: some of these details are obtained from third party information.	2010-01-12	6.8	CVE-2010-0279 XF MISC SECUNIA OSVDB
canon-its -- accessguardian	Cross-site scripting (XSS) vulnerability in Canon IT Solutions Inc. ACCESSGUARDIAN 3.0.14 and earlier, and 3.5.6 and earlier, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to authentication.	2010-01-13	4.3	CVE-2009-4608 XF VUPEN SECUNIA OSVDB JVNDDB JVN CONFIRM
cherokee-project -- cherokee	header.c in Cherokee before 0.99.32 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4489 BID
drupal -- randomizer	Cross-site scripting (XSS) vulnerability in the Randomizer module 5.x through 5.x-1.0 and 6.x through 6.x-1.0, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2010-01-12	4.3	CVE-2009-4602 VUPEN BID CONFIRM
google -- chrome	Google Chrome allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then reading the document.styleSheets[o].href property value.	2010-01-14	5.0	CVE-2010-0315 MISC
hp -- web_jetadmin	Multiple unspecified vulnerabilities in HP Web Jetadmin 10.2, when a remote SQL server is used, allow remote attackers to obtain access to data or cause a denial of service, possibly by leveraging authentication and encryption weaknesses on the SQL server.	2010-01-14	5.8	CVE-2009-4182 BID HP HP
igor_sysoev -- nginx	nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4487 MISC BID BUGTRAQ
microsoft -- windows_live_messenger	A certain ActiveX control in msgsc.14.0.8089.726.dll in Microsoft Windows Live Messenger 2009 build 14.0.8089.726 on Windows Vista and Windows 7 allows remote attackers to cause a denial of service (msnmsgr.exe crash) by calling the ViewProfile method with a crafted argument during an MSN Messenger session.	2010-01-12	4.3	CVE-2010-0278 BID BUGTRAQ
mortbay -- jetty	The Dump Servlet in Mort Bay Jetty 6.x and 7.0.0 allows remote attackers to obtain sensitive information about internal variables and other data via a request to a URI	2010-01-13	5.0	CVE-2009-4609

	ending in /dump/, as demonstrated by discovering the value of the getPathTranslated variable.			MISC
mortbay -- jetty	Multiple cross-site scripting (XSS) vulnerabilities in Mort Bay Jetty 6.x and 7.0.0 allow remote attackers to inject arbitrary web script or HTML via (1) the query string to jsp/dump.jsp in the JSP Dump feature, or the (2) Name or (3) Value parameter to the default URI for the Session Dump Servlet under session/.	2010-01-13	4.3	CVE-2009-4610 MISC
mortbay -- jetty	Mort Bay Jetty 6.x and 7.0.0 writes backtrace data without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator, related to (1) a string value in the Age parameter to the default URI for the Cookie Dump Servlet in test-jetty-webapp/src/main/java/com/acme/CookieDump.java under cookie/, (2) an alphabetic value in the A parameter to jsp/expr.jsp, or (3) an alphabetic value in the Content-Length HTTP header to an arbitrary application.	2010-01-13	5.0	CVE-2009-4611 MISC MISC BUGTRAQ
mortbay -- jetty	Multiple cross-site scripting (XSS) vulnerabilities in the WebApp JSP Snoop page in Mort Bay Jetty 6.1.x through 6.1.21 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under (1) jspsnoop/, (2) jspsnoop/ERROR/, and (3) jspsnoop/IOException/, and possibly the PATH_INFO to (4) snoop.jsp.	2010-01-13	4.3	CVE-2009-4612 MISC
openssl -- openssl	Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_free_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.	2010-01-14	5.0	CVE-2009-4355 CONFIRM CONFIRM VUPEN UBUNTU MLIST DEBIAN SECUNIA SECUNIA SECUNIA CONFIRM CONFIRM
oracle -- database_server	Unspecified vulnerability in the Logical Standby component in Oracle Database allows remote authenticated users to affect integrity via unknown vectors.	2010-01-12	4.0	CVE-2009-1996 CERT
oracle -- database_server	Unspecified vulnerability in the Oracle Data Pump component in Oracle Database 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2010-01-12	4.9	CVE-2009-3411 CERT
oracle -- database_server	Unspecified vulnerability in the Oracle Spatial component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2010-01-12	4.9	CVE-2009-3414 CERT
oracle -- e-business_suite	Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 11.5.10.2, 12.0.6, and 12.1.1 allows remote attackers to affect integrity via unknown vectors.	2010-01-12	4.3	CVE-2009-3416 CERT
	Unspecified vulnerability in the Access Manager Identity			CVE-2010-

oracle -- application_server	Server component in Oracle Application Server 7.0.4.3 and 10.1.4.2 allows remote attackers to affect integrity via unknown vectors.	2010-01-12	5.0	CVE-2010-0066 CERT
oracle -- application_server	Unspecified vulnerability in the Oracle Containers for J2EE component in Oracle Application Server 10.1.2.3 and 10.1.3.4 allows remote attackers to affect confidentiality via unknown vectors.	2010-01-12	5.0	CVE-2010-0067 CERT
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 9.0, 9.1, 9.2MP2, and 10.0 allows remote attackers to affect confidentiality via unknown vectors.	2010-01-12	5.0	CVE-2010-0068 CERT
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 7.0, SP7, 8.1SP6, 9.0, 9.1, 9.2MP3, 10.0MP1, and 10.3.0 allows remote attackers to affect integrity via unknown vectors.	2010-01-12	4.3	CVE-2010-0069 CERT CONFIRM
oracle -- application_server	Unspecified vulnerability in the Oracle Containers for J2EE component in Oracle Application Server 10.1.2.3 and 10.1.3.4 allows remote attackers to affect integrity via unknown vectors.	2010-01-12	4.3	CVE-2010-0070 CERT
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 7.0SP7, 8.1SP6, 9.0, 9.1, 9.2MP3, 10.0MP2, and 10.3.1 allows remote attackers to affect availability via unknown vectors.	2010-01-12	5.0	CVE-2010-0074 CERT
oracle -- e-business_suite	Unspecified vulnerability in the Oracle HRMS (Self Service) component in Oracle E-Business Suite 11.5.10.2, 12.0.6, and 12.1.1 allows remote attackers to affect confidentiality via unknown vectors.	2010-01-12	5.0	CVE-2010-0075 CERT
oracle -- database	Unspecified vulnerability in the Application Express Application Builder component in Oracle Database 3.2.1.00.10 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	2010-01-12	6.0	CVE-2010-0076 CERT
oracle -- e-business_suite	Unspecified vulnerability in the CRM Technical Foundation (mobile) component in Oracle E-Business Suite 11.5.10.2, 12.0.6, and 12.1.2 allows remote attackers to affect confidentiality and integrity via unknown vectors.	2010-01-12	6.4	CVE-2010-0077 CERT
oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 9.0, 9.1, 9.2MP3, 10.0MP2, and 10.3.1 allows remote attackers to affect availability via unknown vectors.	2010-01-12	5.0	CVE-2010-0078 CERT
oracle -- jd_edwards_enterpriseone oracle -- peoplesoft_enterprise	Unspecified vulnerability in the PeopleSoft Enterprise HCM - eProfile component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9 Bundle, #21 and 9.0 Bundle #11 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2010-01-12	4.9	CVE-2010-0080 CERT
orion -- orion_application_server	Orion Application Server 2.0.7 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4493 MISC BUGTRAQ
phpwares -- php_inventory	SQL injection vulnerability in index.php in PHP Inventory 1.2 allows remote authenticated users to execute arbitrary SQL commands via the sup_id parameter in a suppliers details action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party	2010-01-12	6.0	CVE-2009-4595 SECUNIA

	information.			
phpwares -- php_inventory	Cross-site scripting (XSS) vulnerability in index.php in PHP Inventory 1.2 allows remote attackers to inject arbitrary web script or HTML via the sup_id parameter in a suppliers details action.	2010-01-12	4.3	CVE-2009-4596 XF MISC MISC
ruby-lang -- ruby webrick -- webrick	WEBrick 1.3.1 in Ruby 1.8.6 through patchlevel 383, 1.8.7 through patchlevel 248, 1.8.8dev, 1.9.1 through patchlevel 376, and 1.9.2dev writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4492 CONFIRM
sap -- sap_kernel	Unspecified vulnerability in sapstartsrv.exe in the SAP Kernel 6.40, 7.00, 7.01, 7.10, 7.11, and 7.20, as used in SAP NetWeaver 7.x and SAP Web Application Server 6.x and 7.x, allows remote attackers to cause a denial of service (Management Console shutdown) via a crafted request. NOTE: some of these details are obtained from third party information.	2010-01-12	5.0	CVE-2009-4603 MISC SECTRAK BID MISC SECUNIA
sun -- solaris	Trusted Extensions in Sun Solaris 10 allows local users to gain privileges via vectors related to omission of unspecified libraries from software updates.	2010-01-14	6.8	CVE-2010-0310 CONFIRM
varnish.projects.linpro -- varnish	** DISPUTED ** Varnish 2.0.6 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator. NOTE: the vendor disputes the significance of this report, stating that "This is not a security problem in Varnish or any other piece of software which writes a logfile. The real problem is the mistaken belief that you can cat(1) a random logfile to your terminal safely."	2010-01-13	5.0	CVE-2009-4488 MISC BID BUGTRAQ
yaws -- yaws	Yaws 1.85 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	2010-01-13	5.0	CVE-2009-4495 MISC BID BUGTRAQ
zeeways -- zeejobsite	Cross-site scripting (XSS) vulnerability in basic_search_result.php in Zeeways ZeeJobsite 3x allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2010-01-12	4.3	CVE-2009-4601 BID SECUNIA MISC

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bash -- bash	The /etc/profile.d/60alias.sh script in the Mandriva bash package for Bash 2.05b, 3.0, 3.2, 3.2.48, and 4.0 enables the --show-control-chars option in LS_OPTIONS, which allows local users to send escape sequences to terminal emulators, or hide the existence of a file, via a crafted filename.	2010-01-14	2.1	CVE-2010-0002 CONFIRM MANDRIVA

fedoraproject -- sssd	System Security Services Daemon (SSSD) before 1.0.1, when the krb5 auth_provider is configured but the KDC is unreachable, allows physically proximate attackers to authenticate, via an arbitrary password, to the screen-locking program on a workstation that has any user's Kerberos ticket-granting ticket (TGT); and might allow remote attackers to bypass intended access restrictions via vectors involving an arbitrary password in conjunction with a valid TGT.	2010-01-14	3.7	CVE-2010-0014 CONFIRM
oracle -- database_server	Unspecified vulnerability in the RDBMS component in Oracle Database 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2010-01-12	3.6	CVE-2009-3410 CERT
oracle -- application_server oracle -- database_server	Unspecified vulnerability in the Unzip component in Oracle Database 9.2.0.8, 9.2.0.8DV, and 10.1.0.5; and Oracle Application Server 10.1.2.3; allows local users to affect confidentiality via unknown vectors.	2010-01-12	1.0	CVE-2009-3412 CERT
oracle -- database_server	Unspecified vulnerability in the Oracle Spatial component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	2010-01-12	3.2	CVE-2009-3413 CERT
Back to top				

Last updated January 18, 2010



[Print This Document](#)